AGENDA ITEM 3b
FINANCIAL STATEMENT AUDIT MANAGEMENT LETTER COMMENTS
PRIOR YEAR REPORT WITH CURRENT YEAR UPDATES
AS OF JUNE 30, 2010

Audit (Report Issue Date): Report to Management for the Year Ended 06/30/07 (12/14/07)

Observation 14.1: Security Policies and Practices Forms
Division responsible: Information Security Office

Observation:
CalPERS policies state that all newly-hired employees will review the CalPERS Information Security Policies and Practices and sign an Information Systems Security and Confidentiality Acknowledgement (ISSACA) form. In addition, all current employees will review and re-sign the form yearly. The form states, among other items, that the employee agrees to abide by CalPERS information systems requirements including the understanding that:

- CalPERS information assets and computer resources only for CalPERS approved purposes.
- Employees are to access CalPERS systems and networks using only my assigned user identifiers and passwords.

Employees are to notify the CalPERS Information Security Officer immediately of any actual or attempted security violations including unauthorized access; and, theft, destruction, or misuse of systems equipment, software, or data.

While CalPERS policy is that all new-hires complete and sign the ISSACA form and current employees re-sign the form yearly, we found that evidence of the signed forms are not always maintained. Our testing of 18 new-hire forms found that 17 percent could not be found. In addition, we tested six current ITSB employees and were only able to find four completed forms. The lack of available signed forms could indicate that either the employee did not complete the review and subsequently sign the form, or that the form had been misplaced. In either case, the evidence of completion of the form is not available putting the agency at increased risk for non-compliance to the information security policies and practices. CalPERS ISOF (Information Security Office) should institute new procedures to ensure that training is provided and new-hires sign the ISSACA form. Periodic internal reviews should be accomplished to ensure this is being done. In addition, procedures should be implemented to ensure that recurring training is accomplished and the recurring ISSACA form is signed and submitted to the Human Resources Department.

Current Status:
COMPLETE. Pending final verification by Macias, Gini & O'Connell. Information security training is now being delivered via the CalPERS Learning Management System (LMS). The training began March 3, 2010 and as of April 26, 2010, 70% of staff have completed the training. The LMS was procured as a part of the PSR project in order to track and deliver the training necessary to bring CalPERS staff up to speed with the new PSR system. In the last year or so since the LMS went live, it has been integrated into CalPERS as the way all training is scheduled and tracked by the CalPERS All Staff Training and Development (ASTD) section.

The information security training was created by Information Security Office staff, and it is used not only as training, but as a substitute for the paper copies of the ISSACA form. The last few screens of the training replicate the exact text of the ISSACA form, and the final question asks if the staff member agrees to abide by the CalPERS information systems security requirements covered in the course. If the staff member agrees, then they have met the requirement to sign the ISSACA

AGENDA ITEM 3b
FINANCIAL STATEMENT AUDIT MANAGEMENT LETTER COMMENTS
PRIOR YEAR REPORT WITH CURRENT YEAR UPDATES
AS OF JUNE 30, 2010

Audit (Report Issue Date): Report to Management for the Year Ended 06/30/07 (12/14/07)

form. That agreement is recorded by the LMS and it is reported to the Information Security Office. The LMS reports the staff members who have and who have not received the training and who have agreed to abide by the requirements.

Staff members are added to the LMS via a recurring file transfer from CalPERS' PeopleSoft HR system. This insures that all CalPERS staff are registered in the LMS, so that Information Security Office gets a report of all staff who have taken the training and agreed to the requirements.

Observation 15.3: Formal Authorization for User Access
Division responsible: Information Technology Services Branch

Observation:
CalPERS uses an in-house application, Movaris, to manage the workflow used to authorize user account access and authorizations to the various member benefits information systems; CRS, Comet, and RIBS. A review of the process, however, finds that the designated data owners or their formal designees as reported to the Information Security Office, are not required to provide formal authorization prior to a user being allowed access to the application or data. This has the potential to increase the risk associated with the disclosure or integrity of the data as the data owner is not the final approval authority granting access. The CalPERS ITSB should work to ensure that the Movaris application process includes procedures for the formal data owner or the data owner designee to provide approval prior to granting access to an application or data under the responsibility of the data owner. Current user application accounts should also be reviewed by formal data owners to ensure that all accounts currently in use have the proper approvals.

Current Status:
COMPLETE. Pending final verification by Macias, Gini & O’Connell. To comply with the Information Security Office’s “Identity Authentication Practice”, data owner approval functionality has been included in the User Access Request System (UARS) for the COMET, RIBS and CRS applications.

The Information Technology Services Branch has also validated that all current COMET, RIBS and CRS application users have appropriate data owner authorizations. Any user accounts not approved or deemed no longer needed have been removed from the in-scope systems.

Observation 15.4: Shared User Accounts
Division responsible: Information Technology Services Branch

Observation:
Shared accounts are being used by the database administrators when accessing the Oracle database or the VSAM file environment. The use of these shared accounts creates a situation wherein actions taken within the database system cannot be tracked back to a specific individual. Inadvertent or malicious activity may not be able to be positively associated with a specific individual essentially eliminating an effective audit trail.

CalPERS Information Technology Services Branch should evaluate the use of shared accounts

AGENDA ITEM 3b
FINANCIAL STATEMENT AUDIT MANAGEMENT LETTER COMMENTS
PRIOR YEAR REPORT WITH CURRENT YEAR UPDATES
AS OF JUNE 30, 2010

Audit (Report Issue Date): Report to Management for the Year Ended 06/30/07 (12/14/07)

and discontinue their use where it has been determined there is a risk to the database. Database administrator accounts with schema owner access should be controlled with access granted sparingly and only after proper approval has been granted.

Current Status:
COMPLETE. Pending final verification by Macias, Gini & O'Connell. Information Technology Services Branch has completed a review of all non-human IDs with access to VSAM files as well as the Oracle schema owner accounts used by database administrators.

All non-human IDs with access to VSAM accounts have been brought into compliance with the Information Security Office's "Data Owners and Custodians" and "Identity Authentication" practices. Information Technology Services Branch identified two shared accounts with access to VSAM files and facilitated their approval with the appropriate data owners and the Information Security Office. This approval also constitutes the acceptance of risk of their use by both the data owners and Information Security Office.

Information Technology Services Branch also found the risks associated with CalPERS' use of shared Oracle schema owner accounts to have been previously accepted by both Information Technology Services Branch and Information Security Office under Information Security Office's Policy Variance 04-061 dated April 2, 2004.

Observation 15.5: Schema Owner Access
Division responsible: Information Security Office

Observation:
Database administrator with accounts to the Oracle database or the VSAM environments may potentially have the capability to alter member information affecting benefits payments. Tests have not been conducted to determine if the database systems have sufficient logging triggers or oversight such as file balancing or reconciliations to verify if unauthorized changes can be detected.

The CalPERS Information Security Office should conduct testing to determine if persons with schema owner access to the Oracle database or to the VSAM files can make changes to the database that would affect member benefits without detection.

Current Status:
COMPLETE. Pending final verification by Macias, Gini & O'Connell. While database administrators with accounts to the Oracle database or the VSAM environments may be able to alter member information affecting benefits payments, there is a control managed within Member and Benefits Service Branch which reconciles all transaction changes affecting member benefits payments to the individual that made the change.

The BMA054 report is run daily. This report reflects any adjustments to a member's allowance. The report is distributed daily to all supervisors and/or managers to review and sign off on any changes manually keyed by their staff. A master copy of the report is maintained for a year.

AGENDA ITEM 3b
FINANCIAL STATEMENT AUDIT MANAGEMENT LETTER COMMENTS
PRIOR YEAR REPORT WITH CURRENT YEAR UPDATES
AS OF JUNE 30, 2010

Audit (Report Issue Date): Report to Management for the Year Ended 06/30/07 (12/14/07)

Each month a BMA069PI report is run. This report highlights cases which multiple updates to a member's benefits within the same month. The report is distributed monthly to all supervisors and/or managers to review and sign off on any changes made by their staff. A copy of the report is maintained for a year.

Should a database administrator make an unauthorized change to a member's benefits, it would be identified by this control.

Audit (Report Issue Date): Report to Management for the Year Ended 06/30/08 (2/18/09)

Observation 6: Analysis and Reconciliation – GASB 40 and AIM
Division responsible: Fiscal Services Division

Observation:
Our audit procedures revealed numerous errors and inconsistencies in the GASB 40 disclosures, as Fiscal Services did not independently verify whether the amounts provided by the custodian bank were accurate or in conformity with the provisions of GASB Statement No. 40. The original data provided by the custodian bank had a variance of approximately $6 billion which was subsequently addressed and the appropriate data was included in the CalPERS financial statements.

We also discovered errors in the financial statement disclosure of unfunded alternative investment commitments. Certain amounts provided by CalPERS' third party service provider did not agree to information provided by the partners. Although the disclosed amounts were corrected, Fiscal Services did not independently corroborate the unfunded commitments in preparing the financial statement disclosure.

Current Status:
IN PROGRESS. Fiscal Services has received GASB data for CalPERS pooled investments and will send updated procedures and completed third quarter risk disclosure data to Macias, Gini & O'Connell for feedback.

Observation 8: Complete Disclosure of Contingent Losses
Division responsible: Fiscal Services Division

Observation:
We identified a contingent loss that was not properly disclosed in the draft financial statements. Current procedures are not sufficient to ensure that contingencies will be accrued or disclosed in accordance with GAAP.

We recommend that Fiscal Services meet with CalPERS' general counsel to identify pending litigation, claims and assessments in conjunction with the preparation of the annual financial statements and ensure all legal responses are included in the financial statements when appropriate.

AGENDA ITEM 3b
FINANCIAL STATEMENT AUDIT MANAGEMENT LETTER COMMENTS
PRIOR YEAR REPORT WITH CURRENT YEAR UPDATES
AS OF JUNE 30, 2010

Audit (Report Issue Date): Report to Management for the Year Ended 06/30/08 (2/18/09)

Current Status:
IN PROGRESS. Fiscal Services has developed a process for logging and identifying contingent liabilities by virtue of the 2009 Accounting Action Plan. Fiscal Services will institute this process in 2010.

Observation 9: Management's Discussion and Analysis Improvements
Division responsible: Fiscal Services Division

Observation:
Management's discussion and analysis (MD&A) prepared by Fiscal Services meets the minimum GAAP requirements; however, we believe incorporating the unique perspectives of the managers responsible for key activities would enhance the usefulness and improve the users' understanding of the financial statements.

We recommend that Fiscal Services obtain narrative explanations of the significant changes in financial position and results of operation from management responsible for the related activities. Fiscal Services should be heavily involved in the analysis to ensure compliance with the financial reporting standards and to avoid redundancy in the MD&A.

Current Status:
IN PROGRESS. Fiscal Services will continue to prepare separate Word documents of the 2008-2009 Consolidated Annual Financial Report MD&A for submission to appropriate program areas for feedback on suggested revisions.

Observation 13: Password Requirement Non-Compliance
Division responsible: Information Technology Services Branch

Observation:
We found that password requirements used to access the mainframe applications, RIBS and CRS, currently do not fully adhere to CalPERS' Information Security Identity Authentication Practice certain key areas. We recommend CalPERS' mainframe administrator update the Resource Access Control Facility (RACF) security settings to ensure that the settings comply with the Information Security Identity Authentication Practice. The Information Security Office should conduct periodic monitoring to ensure compliance.

Current Status:
IN PROGRESS. The prior year recommendation is in the process of being implemented. With the development and implementation of PSR, it was decided that no further updates to the current legacy applications would take place. As a result, the password configuration requirements were not updated to be in compliance with the I.S. Identity Authentication Practice. This recommendation, however, will be addressed with the PSR system implementation and will replace the mainframe applications, RIBS and CRS.